

Medicaid Medication History Data-Sharing Pilot

Presentation to the NYS DOH Patient Safety Conference

- James Figge, MD, MBA
Medical Director
- New York State Department of Health
- Office of Health Insurance Programs

- May 21, 2007, Holiday Inn on Wolf Road,
Albany, NY



NYS – NYC Medicaid Medication History Pilot

- A component of the \$27 Million NYC DOHMH *Primary Care Information Project*
- Thomas R. Frieden, MD, MPH
Commissioner, NYC DOHMH
- Farzad Mostashari, MD, MS
Assistant Commissioner, NYC DOHMH

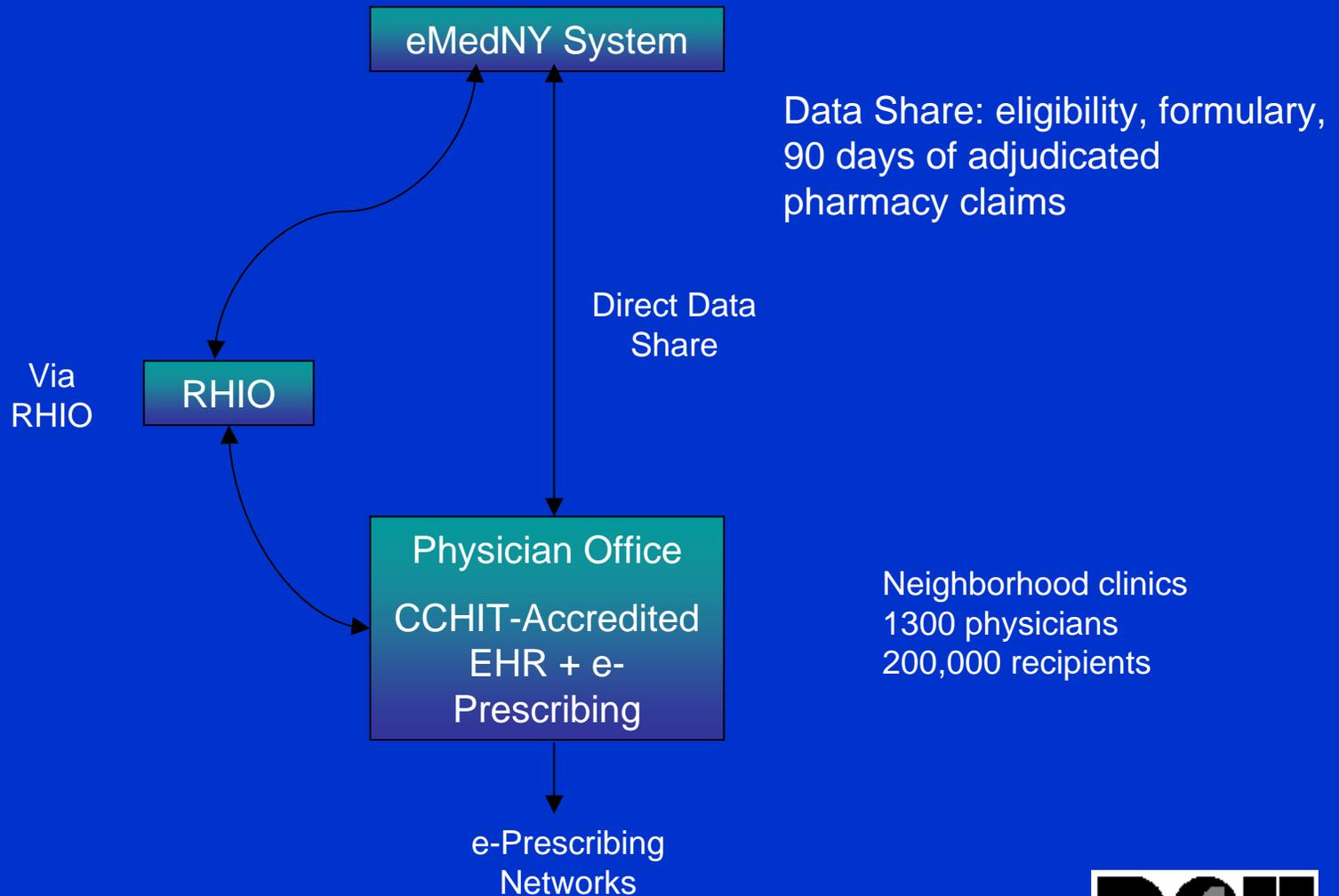


NYS – NYC Medicaid Medication History Pilot

- One year pilot features data sharing of Medicaid Medication History with 1,300 physicians.
- Real time transactions (follows NCPDP SCRIPT, Medicare Part D data standards).
- Eligibility, formulary and medication history.
- 90 days of adjudicated claims.
- Goal is to improve patient safety by enabling decision support, preventing medication errors, and facilitating care coordination and medication reconciliation.
- Written patient consent will be obtained.
- Project evaluation to be conducted.



NYS – NYC Medicaid Medication History Pilot

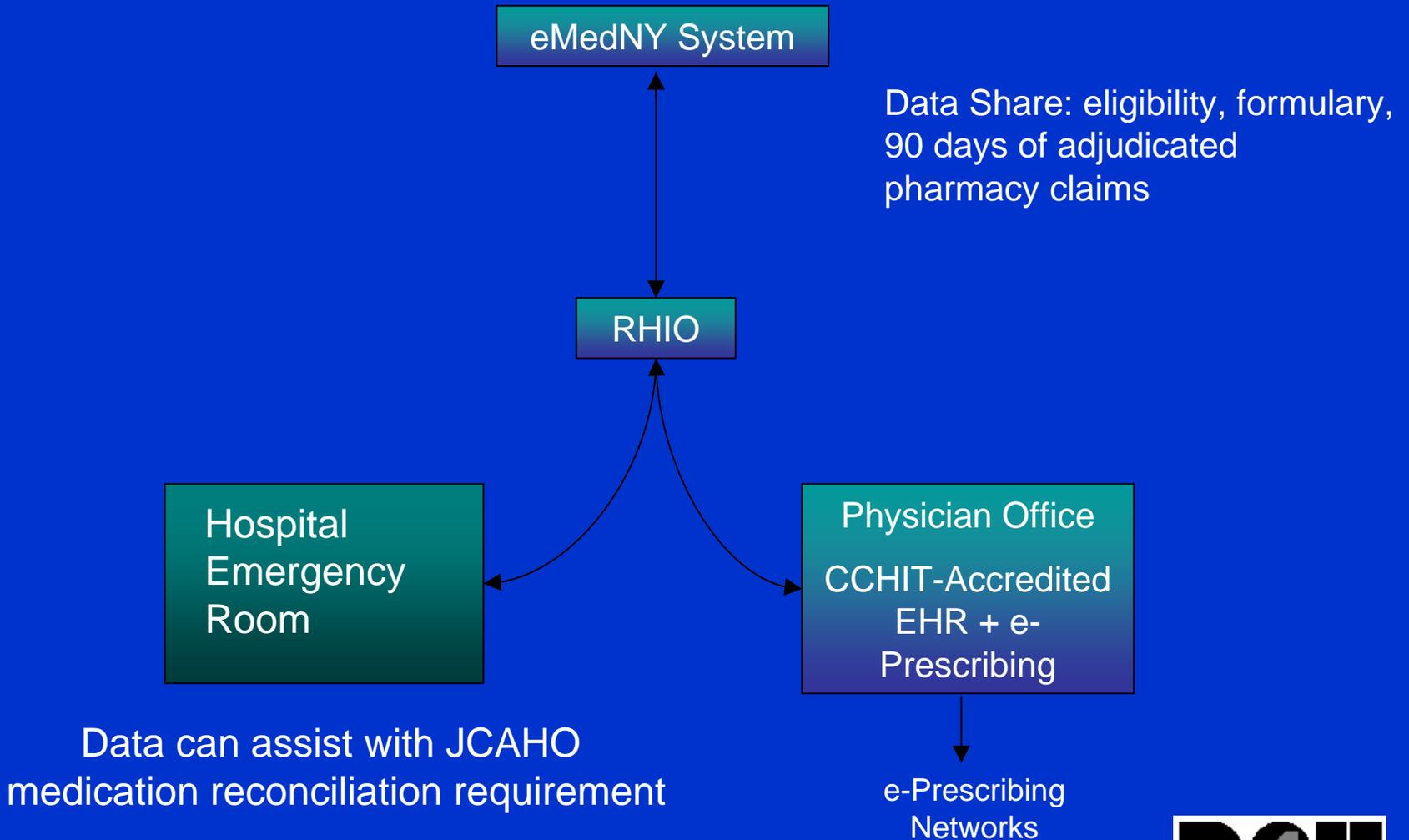


NYS Medicaid Medication History Pilot with Selected RHIOs

- One year proposed pilot features data sharing of Medicaid Medication History with selected RHIOs.
- Real time transactions (follows NCPDP SCRIPT, Medicare Part D data standards).
- Eligibility, formulary and medication history.
- 90 days of adjudicated claims.
- Goal is to improve patient safety by enabling decision support, preventing medication errors, and facilitating care coordination and medication reconciliation.
- Written patient consent will be obtained.
- Technical aspects of data sharing with a RHIO to be piloted.



NYS Medicaid Medication History Pilot with Selected RHIOs



Privacy and Security Standards

- **42CFR 431.303 State authority for safeguarding information.**
- The Medicaid agency must have authority to implement and enforce the provisions specified in this subpart for safeguarding information about applicants and recipients.



Technical Security Standards for Transmission of Protected Medicaid Data via the Internet or Other Open Networks

- Web Services Interoperability Model, conforming to the National Institute of Standards and Technology - Federal Information Processing Standards (NIST - FIPS). Features include:
 - Virtual Private Network (VPN) with tunneling and/or https:// protocol;
 - Triple-DES encryption (*);
 - A hashing algorithm for message authentication (e.g., HMAC {FIPS 198}).

* AES also acceptable



Technical Standards for the Physician's Office

- CCHIT Certified EHR (2006 standards), including user and/or role-based security access privileges, audit records, authentication, data backups, disaster recovery;
- Protection against malicious software (malware / spyware) – the physician's office must present documentation of an active software license with an appropriate vendor covering the time-frame of the pilot program;
- Security certificate to be issued by the State's fiscal agent.



Physical Security

- Safeguards against unauthorized physical access.

